PENDETEKSIAN SERANGAN

MAC ADDRESS DENGAN MENGGUNAKAN WIDS

(WIRELESS INTRUSION DETECTION SYSTEM)

BERBASIS SNORT

SKRIPSI

Oleh :

HANDUNG FIRSTO TAMA
1034010041

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL
"VETERAN" JAWA TIMUR
2014

SKRIPSI

PENDETEKSIAN SERANGAN MAC ADDRESS DENGAN MENGGUNAKAN WIDS (WIRELESS INTRUSION DETECTION SYSTEM) BERBASIS SNORT

Disusun Oleh :

HANDUNG FIRSTO TAMA
1034010041

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Pada Tanggal : 21 Februari 2014

Pembimbing :

1. I Made Suartana, S.Kom, M.Kom.

2. Henni Endah Wahanani, ST., M.Kom.
NPT. 3 7809 130 348 1

Tim Penguji :

1. Dr. Ir. Ni Ketut Sari, MT.
NIP. 19650731 199203 2 001

2. Budi Nugroho, S.Kom, M.Kom.
NPT. 3 8006 050 205 1

3. Achmad Junaidi, S.Kom.
NPT. 3 7811 040 199 1

Mengetahui
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya

Ir. Sutiyono, MT
NIP. 19600713 198703 1 001

Judul	:	PENDETEKSIAN SERANGAN MAC ADDRESS DENGAN MENGGUNAKAN WIDS (WIRELESS INTRUSION DETECTION SYSTEM) BERBASIS SNORT
Pembimbing I	:	I Made Suartana, S.Kom, M.Kom.
Pembimbing II	:	Henni Endah W, ST, M.Kom.
Penyusun	:	Handung Firsto Tama

ABSTRAK

Keamanan jaringan nirkabel atau wireless yang semakin pesat membuatnya rentan dalam sejumlah ancaman keamanan terutama dengan menggunakan metode WIDS (Wireless Intrusion Detection System). Salah satu ancaman keamanan dalam WIDS (Wireless Intrusion Detection System) adalah spoofing ancaman tersebut merubah MAC address.

Pada umumnya MAC address tidak dapat diubah karena sudah ditetapkan oleh NIC (Network Interface Card) dan sudah dimasukkan ke dalam ROM (hardware). Akan tetapi ada beberapa kartu jaringan menyediakan utilitas yang mengijinkan pengguna untuk merubah MAC address, meski hal tersebut kurang disarankan. Perubahan MAC address akan dilakukan untuk memecahkan masalah di atas.

Solusinya peneliti dapat melakukan perubahan MAC address dalam satu ROM (hardware) dan dapat terdeteksi oleh detector. Detector snort disiapkan untuk melakukan analisa serangan MAC address spoofing. Hasilnya dalam analisa, detector snort masih mampu mendeteksi serangan MAC address spoofing dan dengan analisa koefisien cohen’s kappa yang digunakan untuk menghitung reliabilitas antar dua rater. Hasil yang didapat adalah k=0.516 dengan katagori cukup (fair).

Kata Kunci : MAC address spoofing, WIDS, snort

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan segala nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi tepat pada waktunya. Serta atas limpahan rahmat yang tak terhingga penulisan laporan skripsi yang berjudul "Pendeteksian Serangan MAC Address Dengan Menggunakan WIDS (Wireless Intrusion Detection System) Berbasis Snort" dapat terselesaikan.

Skripsi ini dibuat sebagai salah satu syarat memperoleh gelar sarjana komputer di jurusan teknik informatika UPN "Veteran" Jatim. Selesainya skripsi ini juga berkat dukungan semua pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Ayah dan Bunda selaku orang tua yang paling tercinta, terima kasih atas semua doa, dukungan, serta banyak hal lain yang tidak bisa di ucapkan satu per satu, tanpa dukungan dari kalian penulis tidak yakin bisa menyelesaikan skripsi ini tepat waktu. Terima kasih sebanyak-banyaknya atas semuanya. Dan penulis memohon doa agar setelah lulus dari perguruan tinggi dan menyandang gelar sarjana komputer, penulis mampu menjadi lebih bermanfaat bagi orang lain dan dapat membahagiakan keluarga terutama oranga tua.
2. Bapak Prof. Dr. Ir. Teguh Soedarto, MP., selaku Rektor Universitas Pembangunan Nasional "Veteran" Jawa Timur.

3. Bapak Ir. Muttasim Billah, MS., selaku Wakil Dekan Fakultas Teknologi Industri Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Dr. Ir. Ni Ketut Sari, MT., selaku Ketua Jurusan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Bapak I Made Suartana, S.Kom, M.Kom., selaku dosen pembimbing satu. Terima kasih karena telah banyak memberikan arahan, bimbingan, serta meluangkan waktu dalam membimbing penulis untuk mengerjakan skripsi ini.
6. Ibu Henni Endah W, ST., M.Kom., selaku dosen pembimbing dua. Terima kasih karena telah banyak memberikan arahan, bimbingan, serta meluangkan waktu dalam membimbing penulis untuk mengerjakan skripsi ini.
7. Pacarku Holifatus Sofi, terima kasih banyak telah memberikan motivasi dan dukungan dari awal pengajuan skripsi hingga skripsi ini selesai, serta menjadi penghibur hati saat sedang kacau mengerjakan skripsi.
8. Teman-teman seangkatan 2010 Angga, Indra, Genta, Mifta, Bapak Pringga, Davi, Po po, Hamid, dan banyak lagi teman-teman yang tidak bisa di sebutkan satu-persatu. Terima kasih semuanya kerena sudah memotivasi penulis sampai menyelesaikan skripsi ini.

Penulis menyadari skripsi ini masih jauh dari kata sempurna, sehingga saran dan kritik yang membangun sangat berguna bagi penulis. Semoga laporan skripsi ini bermanfaat bagi pembaca dan semua orang yang membutuhkan referensi.

Akhirnya, penulis berharap agar penyusun laporan ini mampu memberikan sumbangsih bagi perkembangan dan kemajuan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.

Surabaya, 21 Februari 2014

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Seiring dengan penyebaran jaringan nirkabel (wireless network) berkaitan dengan komunikasi antar sistem komputer tanpa menggunakan kabel. Jaringan nirkabel ini sering dipakai untuk jaringan komputer baik pada jarak yang dekat (beberapa meter, memakai alat atau pemancar bluetooth) maupun pada jarak jauh (lewat satelit). Bidang ini erat hubungannya dengan bidang telekomunikasi, teknologi informasi, dan teknik komputer. Jenis jaringan yang populer dalam katagori jaringan nirkabel adalah jaringan kawasan lokal nirkabel (wireless LAN/WAN), dan Wi-Fi. Jaringan nirkabel biasanya menghubungkan satu sistem komputer dengan sistem yang lain dengan menggunakan beberapa macam media transmisi tanpa kabel, seperti gelombang radio, gelombang mikro, maupun cahaya infra merah.

Keamanan jaringan nirkabel atau wireless yang semakin pesat membuatnya rentan terhadap sejumlah ancaman keamanan. Jaringan wireless bisa jadi merupakan hal terakhir yang tidak terpikirkan. Pada umumnya bertujuan untuk mendapatkan koneksi internet pada saat connect ke jaringan wireless, akan tetapi banyak juga yang melakukan untuk maksud-maksud tertentu mulai dari keingintahuan, coba-coba, dan research. Salah satu ancaman keamanan dalam wireless adalah spoofing ancaman tersebut merubah IP address dan MAC address. IP addresss (Internet Protocol) merupakan protokol dasar untuk mengirim data melalui jaringan internet dan banyak jaringan komputer lainnya.

MAC address merupakan kode keras pada Network Interface Controller (NIC) dan tidak dapat di ubah. Namun ada alat (software) yang dapat membuat sistem operasi percaya bahwa NIC memiliki MAC address yang dapat memilih sendiri oleh pengguna.

Dari penelitian jurnal, peneliti mencoba melakukan serangan dengan cara memalsukan layanan jaringan nirkabel klien. Dengan menggunakan metode Wireless Intrusion Detection System (WIDS). WIDS merupakan sebuah perangkat lunak ataupun perangkat keras yang digunakan untuk akses yang tidak sah dari sebuah sistem komputer atau jaringan. Dalam penerapannya, metode WIDS (Wireless Intrusion Detection System) menggunakan tools snort-wireless yang berjalan pada sistem operasi linux. Sistem tersebut diuji dengan serangan Man In The Middle Attack berupa ARP spoofing. Paket serangan dapat dilihat melalui monitoring paket berbasis web. (Tasmil, 2012)

Dalam penelitian jurnal sebelumnya pengamanan menggunakan WIDS (Wireless Intrusion Detection System) belum cukup untuk mengamankan serangan, khususnya terhadap serangan ARP spoofing yang menyusup melalui MAC address. Oleh karena itu di dalam sekripsi ini, serangan MAC address akan diperbanyak untuk memaksimalkan pendeteksian serangan. Serangan MAC address nantinya akan dilakukan sebanyak enam puluh kali untuk pengujian serangan agar WIDS (Wireless Intrusion Detection System) menjadi lebih aman dan mampu mendeteksi serangan dari attacker.

1.2 PERUMUSAN MASALAH

Dari latar belakang diatas maka dirumuskan permasalahan dalam tugas akhir ini adalah sebagai berikut:

1. Bagaimana mengimplementasikan detector snort dengan menggunakan virtual?
2. Bagaimana cara mendeteksi serangan MAC address dengan menggunakan tool snort di WIDS (Wireless Intrusion Detection System)?
3. Bagaimana mendokumentasi serangan yang telah dilakukan attacker?

1.3 BATASAN MASALAH

Batasan masalah yang ada di penelitian ini adalah:

1. Detector hanya menggunakan virtual.
2. Serangan menggunakan ARP spoofing yang di fokuskan ke pendeteksian MAC address spoofing.
3. Penyerangan hanya menggunakan satu device.
4. Pendeteksian serangan hanya menggunakan tool snort.
5. Jaringan wireless yang digunakan hanya menggunakan jaringan lokal class C.

1.4 TUJUAN DAN MANFAAT

Adanya tujuan dan manfaat dalam penyusunan skripsi ini sebagai berikut:

1.4.1 Tujuan

1. Dapat mengimplementasikan detector snort dengan menggunakan virtual.
2. Dapat mendeteksi serangan MAC address dengan menggunakan tool snort di WIDS (Wireless Intrusion Detection System).
3. Dapat mendokumentasikan serangan yang dilakukan oleh attaker.

1.4.2 Manfaat

Manfaat yang diperoleh dalam mendeteksi Wireless Intrusion Detection System antara lain :

a. Bagi penulis bermanfaat untuk menerapkan pengetahuan yang di peroleh selama menempuh bangku perkuliahan.
b. Bagi mahasiswa bermanfaat untuk mengenal lebih jauh tentang ilmu pendeteksian di wireless.
c. Bagi pembaca bermanfaat menambah informasi tentang pendeteksian wireless dan sebagai bahan literatur lebih lanjut.

1.5 SISTEMATIKA LAPORAN

Laporan skripsi ini terbagi dari 5 (lima) bab, dimana masing-masing bab terdiri dari beberapa sub-bab yang menjelaskan isi dari bab-bab tersebut. Adapun sistematika penulisan laporan ini sebagai berikut:

1. BAB I PENDAHULUAN

   Pada bab pendahuluan ini menguraikan hal-hal yang berkaitan dengan masalah-masalah yang dihadapi oleh penulis, antara lain: latar belakang permasalahan, perumusan masalah, batasan masalah dan tujuan skripsi.

2. BAB II TINJAUAN PUSTAKA

   Pada bab ini menjelaskan hal-hak yang berkaitan dengan teori antara lain: penelitian terdahulu, landasan teori.

3. BAB III METODE PENELITIAN

   Pada bab ini menjelaskan metode-metode yang dilakukan saat penelitian skripsi berlangsung yang meliputi: rancangan penelitian, rancangan uji coba

dan evaluasi, dan jadwal penelitian (bentuk chart). Rancangan penelitian akan di bagi lagi menjadi: studi literatur, definisi kebutuhan sistem, dan rancangan implementasi.

4. BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang pembahasan sebuah Pendeteksian Serangan MAC address dengan menggunakan WIDS (Wireless Intrusion Detection System) berbasis snort. Mulai dari cara kerja hingga bagian-bagian yang terdapat pada sistem tersebut meliputi: implementasi, hasil uji coba dan evaluasi.

5. BAB V KESIMPULAN

Bab ini berisi kesimpulan dan saran yang sekiranya dapat bermanfaat bagi pembaca.